REMARKS/ARGUMENTS

Claims 96-115 were previously pending in this application. Claims 96, 101, 103 and 107 have been amended. Claims 99, 100, 106 and 111 have been cancelled. Claims 116 and 117 have been added. Consequently, claims 96-98, 101-105, 107-110 and 112-117 remain under consideration. No new matter has been added. Amendment to or deletion of a claim is not to be construed as a dedication to the public of any subject matter.

Claims 96 – 115 are rejected under 35 U.S.C. § 102 (e) as allegedly being unpatentable over U.S. Patent Application Publication No. 2003/0101344 to Wheeler et al ("Wheeler").

Prior to addressing specific claims and specific features thereof in the present application, applicant makes the following general observations regarding the distinctions between Wheeler and the present invention. While Wheeler describes an invention generally making use of public key security, Wheeler's objectives and detailed methods are distinct from the present invention.

Wheeler generally concerns the secure linking of:

information about a public key enabled device

to

the public key of that device.

E.g. see Wheeler [0017].

In contrast, the present invention generally concerns the secure linking of:

a record system pointer

to

a personal authentication device issued to a user

via an anonymous public key certificate.

The present invention is primarily concerned with assuring anonymity of users with respect to record systems containing information about the users. The aim is to *remove* links between a user's identity and their personal information, while preserving the uniqueness of record system pointers.

Wheeler's "PuK-Linked Account Database" contains the public keys of the storage devices (see [0108]). Thus, the database of Wheeler will necessarily contain information identifying the devices. Wheeler emphasizes the need for high security of such a database (e.g. [0022], [0029], [0034]). In contrast, records systems embodying the present invention can be de-identified and do not need to hold (nor secure) any information pertaining to users' public keys, users' identities or users' devices. The objective of the present invention is to enable records systems to contain only de-identified personal information, the personal information being indexed by pointers or the like that are contained in or bound to separate anonymous public key certificates, and the association between the de-identified personal information and the respective individual being verified by the separate anonymous public key certificate.

Furthermore, Wheeler uses keys which are specific to the devices and which are created *before* the devices are assigned to end users; e.g. see Wheeler [0022], first sentence, and Wheeler claim 1 referring to a "public key of a public-private key pair of the manufactured device". In contrast, in the present invention, keys and certificates may be issued to the users and their associated devices *after* the user is associated with their device. Thus the purpose of the certificate(s) in the present invention is to associate, anonymously, the user with a record pointer, the record pointer being for a record system independent of the storage device. In Wheeler, the purpose of the certificate is to associate the device to an account database controlled and/or secured by the device issuer.

More specifically, amended **independent claim 96** includes, among other limitations, "storing an asymmetric cryptographic private key within, and under the control of a portable storage device associated with a registered user, the private key operating within a public key infrastructure," "creating an anonymous public key certificate and storing it within the public key infrastructure, the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key, wherein the anonymous public key certificate contains an electronic record pointer, the electronic record pointer being associated with each item of personal information of the registered user held in the

electronic record system," and "indexing, within the electronic record system, the personal information of the registered user, wherein association of the personal information with the registered user is anonymously verifiable by the electronic record system when presented with and using the anonymous public key certificate and the electronic record pointer, to affect anonymous indexing of the personal information within the electronic record system." Wheeler does not teach any of the above limitations.

First, Wheeler does not teach "storing an asymmetric cryptographic private key within, and under the control of a portable storage device associated with a registered user, the private key operating within a public key infrastructure." While Wheeler discloses that "private key 116 (PrK) is retained within the device 104" ([0107]), Wheeler emphasizes that this occurs "during its manufacture in the facility 102" and "*before* the device 104 is released from the secure environment 114", Wheeler [0107]. Prior to release from the secure environment 114, the device of Wheeler is not associated with a person. Wheeler thus fails to disclose "storing an asymmetric cryptographic private key under the control of a portable storage device associated with a registered user". This reflects the fundamentally different sequence of events required by the Wheeler disclosure as compared with the present invention.

At page 6, third paragraph, the Office Action further asserts that Wheeler teaches "storing an anonymous public key certificate [security certificate is digitally signed by a trusted party to authentication (sic) the device's public key; 112], the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key [0112, 0122 shows the certificate is linked to the public key which is in turn linked to the private key (0107); 0156 shows that the keys are (sic) certificate are all created anonymously and are tied to a device, not a user]". However, it is not the case that the "security certificate" described at [0112] is a public key certificate (and it is nowhere described as such by Wheeler), let alone being an anonymous public key certificate as is required by claim 96 of the present application. Security Certificate SC 126, as seen in Figure 1, is created at Step 608 ([0112], Figure 6) using the device Security Profile 120 [0112]. The purpose of Security Certificate 126

is to enable authentication of the Security Profile of a device [0113]. Wheeler nowhere teaches that Security Certificate 126 has the purpose of retaining anonymity, or should be so configured, or might be put to this use. This is in contrast to the anonymous public key certificate utilized in the present invention, which enables personal information in a record system to be linked to an individual, without losing anonymity.

In contrast, the anonymous public key certificate of the present invention contains a copy of, is bound to, or generally is "associated with an asymmetric cryptographic public key" (claim 96), and is further configured in a way that enables "association of the personal information with the registered user" to be "anonymously verifiable" (claim 96).

Moreover, claim 96 as amended requires that such anonymous verification is effected by inclusion of an electronic record pointer in the anonymous public key certificate. That is, the anonymous public key certificate of the present invention binds the pointer to the authentication (portable storage) device, which in turn carries information binding the device to the registered user, completing an anonymous link between personal information in a record system and the associated individual. The divergent nature of Wheeler's Security Certificate 126 is further illustrated by the fact that the claims and description of the present application nowhere require or disclose inclusion of other "Security Profile" information in the anonymous public key certificate. Wheeler nowhere teaches or suggests that Security Certificate 126 is anonymous or de-identified, nor that it might be used to anonymously bind a record system pointer to a storage device, and in turn to an individual user associated with that device.

The Office Action further asserts that Wheeler [0156] discloses that "the keys are (sic) certificate are all created anonymously and are tied to a device, not a user". Applicant respectfully disagrees. Rather, the "anonymous framework" of Wheeler in [0156] pertains to the distribution of goods and/or services to customers "without regard to any customer-specific information", "on a per device basis", "and are not necessarily on a per customer basis", and "nothing further is required" (see [0142]). That is, Wheeler's anonymous framework does not

relate to storing any personal information of users whatsoever, much less to providing a means for anonymously verifying users' links to any such information. In particular, Wheeler does not teach in their "anonymous framework" that an anonymous public key certificate containing a record pointer can be used to bind that pointer to a storage device associated with the user, with the effect of in turn allowing personal identifying information to be removed from records pertaining to that user from an electronic records system.

With regard to the assertion that "the security certificate is linked to a key pair which are both anonymous" it is again important to note that the "security certificate" 120 of Wheeler is not a public key certificate. Not being a public key certificate, there is no suggestion or disclosure that security certificate 120 could contain a copy of a public key and a digital signature thereof. Accordingly a link, if any, from that "security certificate" to any key pair could only be made indirectly, with Wheeler giving no suggestion of how such a link might be effected as this is not the stated purpose of the SC 126.

Second, Wheeler does not teach "creating an anonymous public key certificate and storing it within the public key infrastructure, the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key, wherein the anonymous public key certificate contains an electronic record pointer, the electronic record pointer being associated with each item of personal information of the registered user held in the electronic record system." Wheeler nowhere discloses that the "security certificate" is a public key certificate, and nor is it. Wheeler merely states that the security certificate must be stored in the device ([0024]), thus failing to teach storage of any certificate whatsoever in a public key infrastructure.

The Office Action at page 6 fifth paragraph further asserts that Wheeler teaches "indexing within an electronic record system personal information of the registered user, whereby association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate [0156; verified because a digital signature is used]".

However, as noted above with respect to paragraph [0142] and [0156], the "anonymous framework" of Wheeler does not record any personal information of users whatsoever. Also as noted previously, Wheeler [0156] does not teach that "association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate", because Wheeler's "security certificate" does not pertain to information about the user in a records system. The present invention teaches that an electronic record pointer or the like included in or bound to an anonymous public key certificate binds that pointer to a cryptographic storage device that holds the matching private key, thereby associating the pointer to a user controlling the device, without otherwise disclosing any identifying information about the user. It is this binding of recorded personal information to key pair and in turn to device that makes association between records and users "anonymously verifiable" as set out in claim 96. It is therefore not the case that the use of a digital signature alone could make the association verifiable, contrary to such assertion in the Office Action.

Furthermore, Wheeler requires "establishing an initial PuK-linked account database" with particular characteristics including high security (e.g. see Wheeler [0022], [0026], [0027], [0031], [0032], claims 1, 8, 10). Such a database is a necessary enabling element which must be present in order for the Wheeler system to be put into effect. In contrast the present invention does not require establishment of any particular enabling database, rather, the present invention can work with one or more existing records systems and relates to a new way of anonymously linking record system pointers to a registered user via a personal device.

Moreover, Wheeler discloses at numerous points the storage of public key in a database, in order to create the linkage in the "PuK-linked account database". (See, for example, [0022] of Wheeler.). That is, a copy of the public key is stored in the database in question.

In contrast, the present invention is concerned with linking a user to a specific record pointer of a record system, in such a way that the record pointer may be presented anonymously (that is, without identifying the user) with assurance that the user was nevertheless involved in

the presentation of the pointer, by way of controlling a storage device in which the pointer has been cryptographically secured. Unlike Wheeler, the present invention at no point involves the storage of any public key in any database. The link between user and record pointer is achieved by storing a copy of the record pointer within a public key certificate. The public key certificate is associated through standard cryptographic means with a storage device registered to the user and controlled by the user, and claim 96 as hereby amended requires that the public key certificate be stored in the public key infrastructure, not a secure database as taught by Wheeler.

Third, Wheeler does not disclose "indexing, within the electronic record system, the personal information of the registered user, wherein association of the personal information with the registered user is anonymously verifiable by the electronic record system when presented with and using the anonymous public key certificate and the electronic record pointer, to affect anonymous indexing of the personal information within the electronic record system." In the final Office Action at page 4 final four lines and page 5 first paragraph, the Examiner contends that [0140-0141] of Wheeler address the feature of the present invention of "indexing, within the electronic record system, personal information of the registered user, whereby association of the personal information with the registered user is anonymously verifiable by use of the anonymous public key certificate". The Examiner contends: *"When a device is associated with a user there is an index which points to a user's account (0141). The association of the personal information of the user is always verifiable through use of the private key. In other words, when the anonymous private key is used to sign a message, the public key which relates to the private key can be linked to the account through the secure database.*" Applicant respectfully disagrees.

However, what is referred to in the above description of Wheeler is the index of an account database, the database created for the purpose of supporting the issuance of devices to registered users. Wheeler's invention is thus limited to a very narrow purpose, namely linking a public key to the index in the account database. In contrast the present invention as set forth in claim 96, provides elements distinct from Wheeler which enable an anonymous public key certificate to be related to record pointers in practically any type of record system, such other

systems being altogether independent of any account database, and importantly to provide anonymous indexing of such diverse systems. The linkage in the present invention is between a record pointer used in the external record system and the registered user's device. Because the device account database focused upon by Wheeler is not logically connected to an external record system, no index in the account database has any relationship with any external record pointer.

Also, Wheeler fails to disclose or suggest a method for "indexing, within the electronic record system, the personal information of the registered user, wherein association of the personal information with the registered user is anonymously verifiable by the electronic record system." As set out in the preceding, the PuK secured account database of Wheeler cannot be considered to be an electronic record system requiring the benefits of the present invention, the nature of such record systems being set out at pages 2 line 13 to page 3 line 6 of the present specification, for example. Rather, the database of Wheeler is a high security store of users' Public keys and a tool to enable the very distinct methodology of Wheeler.

Moreover, the database of Wheeler is in no way anonymously indexed. First, the contents of Wheeler's database are the devices' public keys and a linked Security Profile of each device (e.g. see Wheeler abstract, [0022], [0027], [0032], claims 1 & 10), which destroys anonymity of the device, because inspection of such database contents immediately enables identification of the associated device, by reference to the Security Profile. Wheeler fails to disclose any de-identified (anonymous) database or record system whatsoever. In contrast, anonymous indexing is essential to the present invention, in that the electronic record does not identify the associated user, the user's public key, nor the device issued to that user. Rather, the device contains an anonymous digital certificate which contains a pointer value (but no identifying information of the user), thereby enabling anonymous verification of the link between the user, the device, and the electronic record containing the user's personal information.

Additionally, with respect to the limitation of "affect anonymous indexing of the personal information within the electronic record system," in the amended claim 96, the principles taught by Wheeler cannot be applied to achieve anonymous indexing of an external record system, being any record system separate from the account database of the device issuer, as is affected by the present invention. This is made clear when considering crucial differences between Wheeler and the present invention. Firstly, the "security certificate" of Wheeler [0024] generally associates a "Security Profile" of a device to a public key of the device. Secondly, the Security Profile of Wheeler contains information about the device and not about the user of the device. ([0017]). Wheeler discloses creating a public key certificate that links device information. Additionally, the Security Profile of Wheeler may include security features, security characteristics, authentication capabilities and manufacturing history (see Wheeler Fig 19).

Nowhere does Wheeler disclose including in the Security Profile nor the Security Certificate any personal information of the user, in particular a record pointer relating to the user in any external database separate from the device issuer (e.g. [0024, 0112, 0121]). In contrast, the certificate of the present invention as claimed in amended claim 96 combines a record pointer and a public key, and has the combination digitally signed. This links the public key to a record pointer, not to a device security profile, and has a different effect from Wheeler; namely, the present invention provides the means for the device holder to prove their association with a record pointer of an external record system, independent of the device issuer, in order to anonymously access that record system.

Wheeler does not teach that a public key certificate linked to a user and a device can contain a record pointer for another record system, independent of the device issuer, wherein the device can be used to present a cryptographically secure value of the record pointer in order to access the record system.

We further provide here a clear illustration of the difference between Wheeler and the present invention, as may be seen in Wheeler Figures 17-18 and associated parags. [0131-0136].

Here Wheeler discloses a third party 1732 acting as "Account Authority" with account database 1738. The third party can be a medical provider [0132]. Devices 1804 are manufactured and earmarked [0133] for the third party Account Authority and distributed to users 1736. Wheeler makes a point at [0132] of stating that "*each database record for the customer 1736 typically is indexed within the database 1738 by a unique account number*". We note that Wheeler makes no further reference to the account number in discussing the embodiment in [0131-0138]; that is, Wheeler's invention does not concern itself with the account number that indexes the database 1738. In contrast, the present invention is primarily concerned with such matters as account numbers of users in third party databases such as 1738 in Wheeler Figure 17.

Indeed, the present invention could be applied to safeguard such account numbers by modifying Wheeler's Figures 17 & 18 to effect the present invention. Account Database 1738 appears in Wheeler Fig 17 in relation to third party Account Authority 1732. Electronic Communications (EC) are sent by users to Account Authority 1782 in which a Message M is digitally signed (DS) by a private key in the device 1804. Database 1738 involves account numbers that uniquely relate to users 1736. Assume for this example that the database contains records indexed by account number. To reliably and anonymously present account numbers when a user wishes to access a record system such as the account database 1738, an additional transaction from 1782 to 1736 is required and is taught by the present invention but not by Wheeler. This transaction would, in accordance with the present invention, deliver the public key certificate containing the Public Key and the record pointer (in this example, being the account number) into the storage device of the user when initially setting up the device for the user. In accordance with the present invention, this would link the public key to, in this scenario, the Account Number of the user. Then when the user wishes to, say, create a new record entry, the new record entry would be sent from user 1736 to the account database 1738 together with a digital signature. The digital signature would, in accordance with the present invention, be constructed from a private key operating on the new record entry. The new record entry and the

signature thereof would consequently be verifiable by the account number certificate of the current invention, rather than by any Security Profile certificate such as that of Wheeler.

As is evident from Figs 17 and 18, neither such transaction is disclosed or suggested by Wheeler, but in contrast is provided by the present invention as set forth in claims 96, 103 and 115. We trust that this example assists to further illustrate the distinctions of the present invention over the teachings of Wheeler.

As a result, for at least any of the above reasons, amended claim 96 is not anticipated by Wheeler and therefore is patentable over the cited references.

Amended independent **claim 103** includes, among other limitations, " an electronic storage for indexing personal information of a registered user; and a portable storage device for a registered user, an asymmetric cryptographic private key being within and under the control of the portable storage device, the portable storage device being provided with information for associating the registered user with the portable storage device; and the portable storage device storing an anonymous public key certificate associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key, the anonymous public key certificate containing an electronic record pointer, the electronic record pointer being associated with each item of personal information of the registered user held in the electronic record system; wherein association of the personal information with the registered user is anonymously verifiable by use of the anonymous public key certificate and the electronic record pointer to thereby effect anonymous indexing of the electronic record system." As explained above, with respect to claim 96, Wheeler does not disclose the above limitations.

Accordingly, amended claim 103 is not anticipated by Wheeler either and therefore is also patentable over the cited references.

Independent **claim 115** includes, among other limitations, "the portable storage device being provided with information for associating the registered user with the portable storage

device, wherein an asymmetric cryptographic private key is under the control of the portable storage device, wherein an anonymous public key certificate is associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key, and wherein association of anonymously indexed personal information with the user is anonymously verifiable by use of the anonymous public key certificate." As discussed above, with respect to claim 96, Wheeler does not teach the above limitations.

Consequently, independent claim 115 is not anticipated by Wheeler either and therefore is also patentable over the cited references.

Dependent **claims 101 and 107** include the additional limitation of "wherein digital signature codes verifiable by using the anonymous public key certificate are created for new data items written into the electronic record system, in order to explicitly link each digitally signed data item to the electronic record pointer contained within the anonymous public key certificate, and wherein each digital signature code is interpreted as explicitly recording the consent of the registered person associated with the record pointer to the creation of each respective digitally signed data item." As explained above, Wheeler does not teach the above limitation. That is, the use of digital signatures are for entirely different purposes of any digital signatures disclosed by Wheeler and not "for new data items written into the electronic record system, in order to explicitly link each digitally signed data item to the electronic record pointer contained within the anonymous public key certificate," as recited by dependent claims 101 and 107.

Therefore, dependent claims 101 and 107 are also allowable over the cited references, as being dependent from allowable independent claims 96 and 103, respectively and for the additional limitations they include therein.

Dependent **claims 102 and 108** include the additional limitation of "wherein digital signature codes are created for given data items in the electronic record system using the asymmetric cryptographic private key, where each digital signature code is interpreted as

explicitly recording the consent of the registered person to the creation of each respective digitally signed data item." Again, there is no teaching or even suggestion in Wheeler about the above limitation.

Accordingly, dependent claims 102 and 108 are also allowable over the cited references, as being dependent from allowable independent claims 96 and 103, respectively and for the additional limitations they include therein.

Dependent **claim 114** includes the additional limitation of "wherein the authorized user is a health care professional authorized by the registered user to enter an update to the registered user's indexed personal information." However, Wheeler nowhere mentions a medical health records database containing user personal information to be updated by health care professionals. The reference at [0132] of Wheeler to a "medical provider" is to merely list a medical provider as one type of service provider who may establish an accounts database. As noted previously herein, Wheeler nowhere discloses de-identified record systems of any description, let alone a medical health records database.

Therefore, dependent claim 114 is also allowable over the cited references, as being dependent from allowable independent claim 103, and for the additional limitations it includes therein.

In short, independent claims 96, 103, and 115 define a novel and unobvious invention over the cited references. Dependent claims 97-98, 101-102, and 116-117; and 104-105, 107-110, and 112-114, are dependent from claims 96 and 103, respectively and therefore include all the limitations of their respective independent claims and additional limitations therein. Accordingly, these claims are also allowable over the cited references, as being dependent from allowable independent claims and for the additional limitations they include therein.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By _____
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clm

CLM PAS948204.1-*-03/15/11 11:59 AM